1

Overview

A brief summary of IBM Managed Security Services and the business challenges addressed

2

Deployment

A look at the IBM solution, including its capabilities, technical components, and cost

3

Service Delivery

How IBM will manage your security assets, monitor your environment, analyze event data and handle security incidents

4

Support and Reporting

Our customer portal, problem management and the query and reporting tools that can help you manage your security environment

5

Next Steps

Steps you can take and resources you can explore to learn more about IBM Managed Security Services

1. Overview

The need for protection

Enterprises of all sizes struggle in an ongoing battle to defend against online attackers that can strike at any moment. Whether it's a virus or denial-of-service attack or unauthorized database access, successful security attacks wreak havoc by disrupting business operations, reducing workforce productivity, damaging the infrastructure and harming reputation and brand value. Liabilities associated with inadequate security management are becoming more severe, ranging from resources required to remedy the breach, costly downtime and potential loss of business to penalties for regulatory noncompliance.

While IT security threats continue to evolve, organizations face shrinking budgets, competing priorities and more complex environments. Today's IT security departments need to deliver a higher level of protection at a significantly reduced cost.

However, organizations managing their own information security often lack the in-house resources required to protect online systems on a 24x7x365 basis. Advanced security practices require highly skilled personnel who can be expensive to recruit, hire and retain. In addition, implementing and managing security solutions can divert IT resources from other critical initiatives, including preventing the next attack.

IBM Managed Security Services

IBM Managed Security Services for customer premises equipment (see Table 1) are designed to provide around-the-clock, near-real-time monitoring and management of security technology from a variety of vendors, helping you protect the value of your existing security investments while reducing the complexity and cost of your security operations.

These managed services can be employed individually or in combination to help organizations:

- Improve security posture and mitigate risks to business operations

- Reduce the cost of security management
- Simplify management and reduce complexity
- Address critical skill shortages
- Support compliance management.

IBM also offers a comprehensive range of hosted managed security services as well as a IBM Managed Web Defense solution. By combining offerings from IBM's full portfolio of complementary managed services, you can increase both your cost savings and your security intelligence. That's because IBM's global security operations infrastructure is designed to integrate data from multiple managed security services, helping you to bridge IT

Firewall Management—24x7 firewall monitoring, escalation, incident reporting, and remediation assistance.	
• Check Point NGX / R71 and later	• Cisco • Juniper Netscreen
Unified Threat Management—24x7 management with support for comprehensive UTM product features (firewall, IPS/IDS, anti-virus, anti-spam, web filtering, SSL VPN).	
• IBM Proventia® Network Multi-Function Security • Check Point UTM-1, Edge and IP Appliance	• Cisco ASA, ISR • Juniper SSG, ISG + IDP, SRX • Palo Alto Networks • Fortinet FortiGate
Intrusion Detection and Prevention Management—24x7 threat monitoring, escalation, incident reporting, and remediation assistance.	
• IBM Proventia G, GX, XGS, VSP • IBM Security Server Protection • Cisco IDS, IPS, IDP • Juniper IDP • McAfee Intrushield, M Series IPS	• SourceFire • FireEye NX Series • Check Point IPS-1 • TrendMicro Deep Security IPS
Managed Security Information and Event Management (SIEM)—Provides 24x7 expert monitoring and response for customer SIEM tools.	
• IBM Q1 Labs® QRadar®	• HP ArcSight
Managed Secure Web Gateway and Email Security—Ongoing protection of critical web-based transactions.	
• BlueCoat SG (Proxy) • BlueCoat AV (w/SG)	• WebSense Web Security Gateway • FireEye NX Series, EX Series
Managed Protection Services—24x7 protection and live, expert management, monitoring and escalation for enterprise networks and endpoints. **Vulnerability Management Services**—Ongoing security scans that help identify and prioritize vulnerabilities found on network devices, operating systems, web applications and databases.	

Table 1. IBM Managed Security Services (customer premises equipment) and device support

silos and technologies and gain an end-to-end view of your security landscape (see Figure 1). The end result is more information, correlated by IBM in near real time for deep analysis and faster response to threats.

Service features

IBM Managed Security Services offer industry-leading tools, technology and expertise combined with flexible, scalable packaging to meet a broad range of requirements. Whether you purchase managed services for one or for multiple device types, your security solution will include:

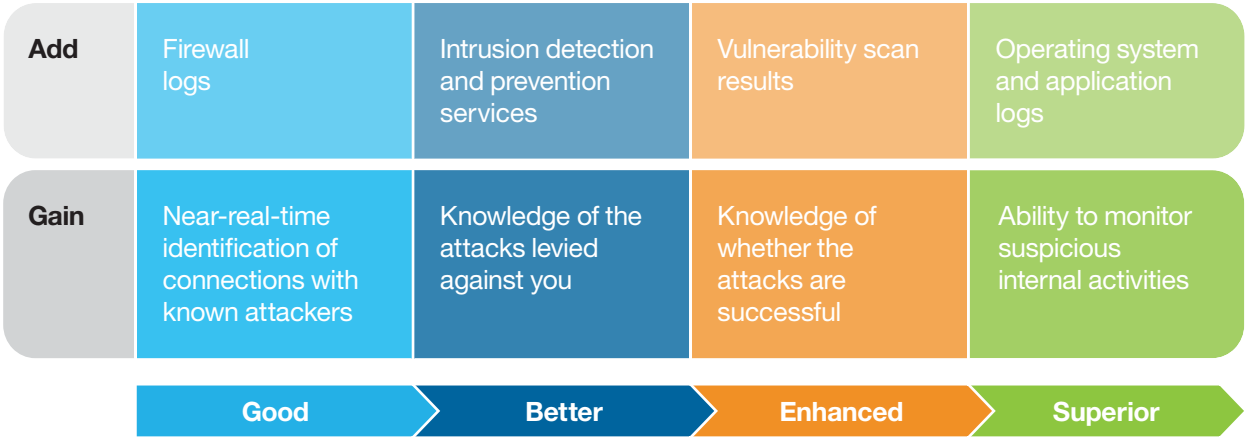

Figure 1. Combining IBM Managed Security Services offerings can help increase your analytic capabilities.

After classification, the SOC analyst prioritizes the incident by correlating three factors (see Figure 6). Security incidents are assigned to one of three priority levels:

- **Priority 1:** Incidents at this level are actionable, high-risk events that have the potential to cause severe damage to customer environments. Priority 1 events require customers to take immediate defensive actions. System or data compromises, worm infections and propagation, massive denial of service (DOS) attacks, and similar incidents are assigned this priority level.
- **Priority 2:** This is the lowest level of actionable incidents. Priority 2 incidents require customers to take actions within 12 to 24 hours of notification by the SOC. Incidents such as unauthorized local scanning activity and attacks targeted at specific servers or workstations are assigned this priority level.

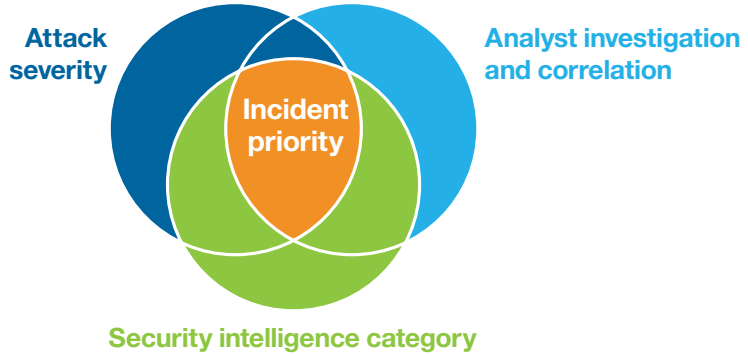

Figure 6. SOC analysts prioritize incidents based on three criteria.

- **Priority 3:** Incidents in this category involve activity on a network or server that is not directly actionable. Discovery and vulnerability scanning, information gathering scripts and other reconnaissance probes are assigned this priority level.

Phase 4: Incident escalation

Once an incident has been identified, classified and prioritized, IBM escalates it to your authorized security staff for handling. Contracted service levels determine how quickly security incidents will be escalated, with service level options for 15-, 30- or 60-minute response times. Customers can set preferences for preferred methods of notification—for example, telephone, mobile phone, email or via the portal. During a Priority 1 security incident escalation, IBM will attempt to reach the designated customer contact until successfully notified or all escalation contacts have been exhausted.

Phase 5: Countermeasure recommendations

After reaching an authorized contact during a Priority 1 security incident escalation, the SOC analyst will recommend appropriate actions to thwart or contain the attack. The countermeasures available to the SOC and clients vary based on the services and platforms managed by IBM at the affected site. A list of countermeasures and their associated properties is detailed in Table 2.

Countermeasure Type	IBM Default Action	Requires Authorization	Platforms
Reactive Block	No	Yes	IBM IDS/ IPS
Kill	No	Yes	All network and host IDS/IPS
ISP notification	Yes	No	All
Firewall policy or ACL change	No	Yes	IBM IDS/ IPS or managed firewall

Table 2. SOC analysts will work with you to determine actions you can take to thwart or contain an attack.

Important note: *The client Incident Response Team is responsible for verifying and acting on SOC-escalated incidents, in accordance with the organization's Computer Security Incident Response Plan (CSIRP). As your team executes your CSIRP, it is critical that you and the IBM SOC staff remain in close communication. For its part, the SOC will continue to provide assistance and offer recommendations where appropriate. If your organization lacks a robust CSIRP or an emergency response capability, IBM offers security consulting services that can address your particular needs.*

Phase 6: Documentation

The final stage of any security incident escalation is documentation. All aspects of the activity and attack are documented within a security incident ticket and report. Ticketing and reporting information is available to customers in real time via the Virtual SOC customer portal.

IBM Security by the numbers

133+ monitored countries (Managed Security Services)

3,300+ service delivery experts

20,000+ devices under contract

270,000,000+ endpoints protected

20,000,000,000+ events managed per day

4. Support and Reporting

Virtual SOC customer portal

The Virtual SOC customer portal is a web-based portal that serves as a centralized command center for monitoring and controlling security devices under IBM management. It is available online 24x7x365 from a desktop or handheld device. The portal may be used to submit policy change requests, create tickets, generate reports and view security events and logs from managed devices at a single location. With the Virtual SOC portal (see Figure 7):

- Consolidated security views enable monitoring and control of all managed security services via a centralized command center and the viewing of all security events and logs through a single tabbed interface.
- Powerful query and reporting options allow ad hoc queries and reports for security devices, security events, service level agreement activity and other parameters as well as customized standard reports.
- Event/log archives provide online event/log storage accessible via the Virtual SOC portal and offline archiving in the forensically sound IBM Managed Security Services archive system.
- A granular permissions system allows you to determine who can access the portal, what each user sees, what each user can change, and who is authorized to contact the SOC.
- Integrated trouble ticketing and workflow provides a trouble ticket workflow system for the creation, assignment and tracking of ticket status.
- Integrated X-Force security intelligence includes real-time integrated X-Force security intelligence feeds and research tools.

Problem management and resolution

The process for managing security incidents is detailed in Section 3 of this guide. Service incidents—problems outside of standard service operations that cause, or may cause, a reduction in service quality or a security compromise—are addressed by a separate team of SOC specialists. Both types of incidents are tracked end-to-end via the integrated ticketing system.

Service incidents classified by customers as major (Severity 1) pose a risk to critical business processes, such as revenue generation, or result in an outage to a system, network or key application that

Figure 7. The Virtual SOC portal provides a single point of access to all aspects of Managed Security Services delivery.

impacts IT service delivery. Major incidents are handled with an expedited process designed to restore normal operations as quickly as possible. SOC incident management specialists work with the customer through resolution of the problem, and at any time customers can escalate problem handling to the SOC team lead or shift manager.

Trouble tickets can be opened for lower priority incidents either by automated systems and monitoring functions, by SOC personnel or by customer security contacts. These problems are routed to the appropriate SOC operations support teams for resolution.

X-Force security intelligence

Included with all IBM Managed Security Services, and integrated into the Virtual SOC portal, is the IBM X-Force Threat Analysis Service. This industry-leading security intelligence service helps you proactively manage daily security threats by providing an evaluation of global online threat conditions and detailed analysis tailored for your needs. Figure 8 shows a typical client view of the X-Force Threat Analysis home page on the Virtual SOC portal, which provides at-a-glance access to:

- **Current Security Assessment:** a summary of the important events and product releases that could impact your network security
- **Vulnerabilities:** a customized matrix that shows the number of vulnerabilities, by category, over the last 90 days and since your last portal login as well as trends across all available vulnerability data

- **AlertCon 5-Day Forecast:** an assessment of the current and anticipated threat level of online attacks, ranging from AlertCon 1 (regular vigilance required) to AlertCon 4 (catastrophic threat imminent or ongoing)
- **Alerts/Advisories:** a timely compilation of breaking information on new threats from both IBM and from US-CERT
- **Worms & Viruses:** the top three worms and viruses active on the Internet
- **Security News:** an aggregated view of the top security news stories compiled by XFTAS, with links to a news archive.

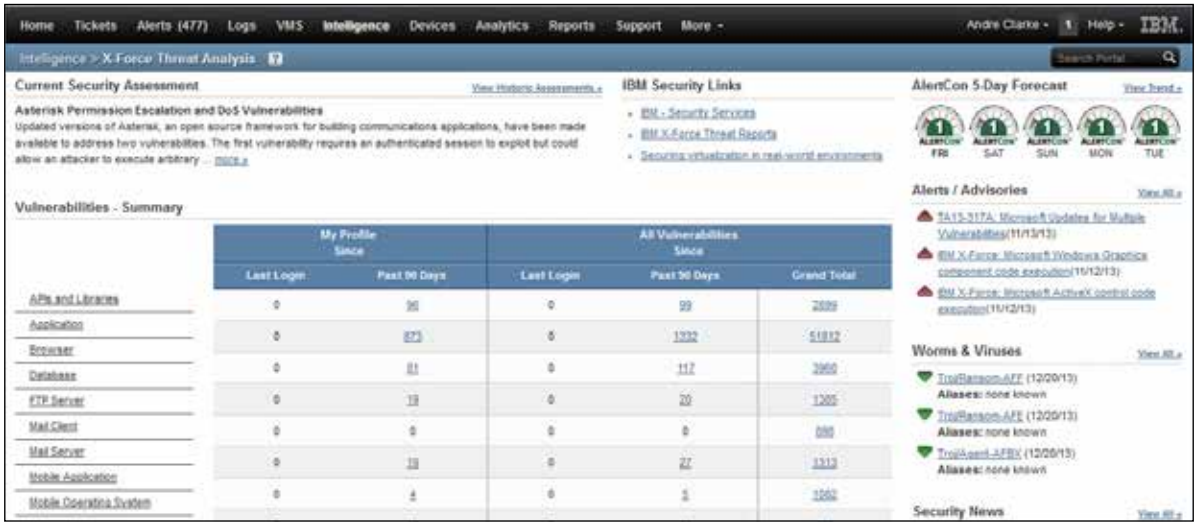

Figure 8. The X-Force Threat Analysis Service home page provides an at-a-glance view of vulnerability trends, Internet security status and your customized security assessment.

Email notification of threat assessments and alerts

As an XFTAS customer, you can subscribe to daily newsletters that provide insightful information about the day's issues, emerging threat trends and their impact, and a tailored list of vulnerabilities, threats, and news articles that pertain to your business. You can also subscribe to a customizable daily threat assessment e-mail that includes IBM protection advisories and daily AlertCon status, which indicates the current threat state of the Internet.

Standard and customized reports

IBM provides a robust reporting and query engine that you can use to help facilitate day-to-day security operations, including research, vulnerability assessment, threat mitigation, and workload prioritization. There are also reports that can help you manage your IBM services and address audit compliancy requirements. IBM provides normalized data from your IBM services and devices managed and monitored by IBM.

Reports are available 24x7x365 through the Virtual SOC portal Report Dashboard (see Figure 9). IBM provides several industry-standard report templates that you can customize by device, device group or time frame to match your requirements. In addition, you can save your report criteria and schedule reports to automatically run hourly, daily, weekly, monthly or yearly. You can view report data directly in the portal or export reports and email them to your security community in HTML, CSV, PDF or other commonly supported formats.

- **Firewall:** Detailed data related to network traffic, protocol usage, connections, target IPs, rule utilization, and suspicious host correlation
- **Log Management:** System activity data for clients using the Hosted Security Event and Log Management Service
- **Alerts:** Summaries of potential security issues and corresponding counts
- **Content Management:** URL filtering (what was blocked by category, by client and source IP) and anti-virus reports
- **Compliance Reports:** Documentation of performance in meeting regulatory, industry and legal standards.

As a best practice, IBM recommends that clients regularly run and review event count reports, in particular event counts by IP source address, by event name and by sensor. Together these reports can help you quickly determine whether attacks are coming from within or outside of your organization, what systems may be compromised, which types of attacks are most prevalent, and which devices may need additional policy tuning.

5. Next steps

IBM specialists can work with you to create a business case that demonstrates how IBM Managed Security Services can help you improve your security posture and mitigate risks to business operations while reducing the cost and complexity of security management.

Contact us

If you would like to speak with an IBM Security Services representative to discuss your security management requirements and objectives, contact us directly by calling 1-877-426-3287. Mention code 609CG98W (U.S. and Canada only). Or you can email us to request a response from an IBM specialist.

Learn more

Read about the issues facing IT security executives today and how IBM can help you address your most significant challenges.

Download the IBM Security Services Cyber Security Intelligence Index to learn more about the threats facing your organization today.

Read the Forrester report Surviving the Technical Security Skills Crisis for an analyst view on the role of managed security services in helping to close the skills gap.

Share the Chief Information Security Officer (CISO) report A new standard for security leaders from the IBM Center for Applied Insights.